SECURITY NOW!

Transcript of Episode #331

Mega Security News Update

Description: We had so much news this week that it squeezed out our show's planned topic of Google's new SDPY web browser protocol. So we'll tackle that early next year. In the meantime, Leo and Steve will discuss the news of this very active week!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-331.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-331-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 331, recorded December 14th, 2011: Mega Security News Update.

It's time for Security Now!, time to cover your security and privacy needs online. And who better than - what do they call you? What does Consumer Reports call you? The master security technician?

Steve Gibson: Apparently "mastermind security expert."

Leo: A mastermind.

Steve: Someone tweeted that. I knew that we had appeared in Consumer Reports. This is, by the way, is the Password Haystacks page, which has been just an amazing amount of value for the amount of time I spent. It demonstrates to me that there's not a linear relationship between how much time I spend on something and what it ends up yielding.

Leo: No. Bloggers have known that for years, that you'll do an offhand post that gets millions of hits, and then you'll work days on a post that gets nothing. And it really is not related to how much work you put into it, but in fact to, I think, and this is a good example, general interest. And there's a lot of general interest in how to make passwords more secure. But before we say that, hello, Steve Gibson.

Steve: Well, Leo, welcome back from Paris.

Leo: Thank you.

Steve: Tom and I had, well, I wouldn't say we had fun without you, but we survived.

Leo: No, you can have fun without me.

Steve: We survived. I participated in TWiT on Sunday. It was...

Leo: Thank you for doing that. I really appreciate that.

Steve: ...extra fun. And in fact I have you this week, not next week. But the cool thing is, for the people who have been excited about our Holiday Sci-Fi Special Edition, we will be live and recording it at our regular time on December 28th.

Leo: So the 21st I will not be here.

Steve: Right.

Leo: But because it's - I'm going to take some holiday time off next week.

Steve: That'll be your holiday time.

Leo: Yeah. And then the following week we're going to do a special, which will be a lot of fun, covering...

Steve: Science fiction.

Leo: Science fiction, one of our favorite nonsecurity subjects, frankly.

Steve: Yup. Movies, TV, and books.

Leo: And so that's the special. That's a special on a very special Security Now!.

Steve: A Holiday Sci-Fi Special Edition.

Leo: Now, but you were mentioning this Consumer Reports thing. I have found it, by the way, online.

Steve: Yeah. If you put in, like, "Consumer Reports Password Haystacks," bang, it takes you right there.

Leo: Yeah. And they have a picture of you. Let me see - I've got to show this.

Steve: I don't know where they got that. I know...

Leo: That is a young Steve Gibson.

Steve: Yes. And those are SGI monitors that were unbelievably advanced at the time. They were 1600x1200. And this was a Newsweek photographer who came out. So I don't know how they found that Newsweek image, or where. Maybe it's images.google.com? There's a lot of me there. But anyway, I was sort of surprised. It's like, oh, yeah, I remember when that was taken, but I don't know how Consumer Reports got a hold of it.

Leo: So here are three techniques for creating strong passwords and remembering them: Use a sentence; use a passphrase; and then yours, growing the haystack. "Developed by security expert Steve Gibson, president of California-based Gibson Research" - with a link. With a link? That's nice. Thank you, Consumer Reports. "Growing the haystack takes" - they must listen to this show. They have quite a good amount of detail in here.

Steve: Yeah, it's a great report. Now, somebody tweeted that somewhere the word "mastermind" was used, so I did a quick Ctrl-F for "find" and put in "master," and it's not on that page. So maybe it's in the print edition, which he said was January 12th was the date in my Twitter stream. So anyway, that's what sort of brought this...

Leo: Yeah, there may be print edition later on. But that's great.

Steve: Yeah.

Leo: It's nice that you're getting recognized. In fact, that's the - boy, you've gotten recognized for that more than anything you've done in the last 10 years.

Steve: I know. It's, I mean, been amazing.

Leo: Yeah. Well, well done, Steve Gibson. Well done, my friend. Moving on.

Steve: Yes.

Leo: Actually, before we move on, this is - let's describe this show because it's a little bit of a change here.

Steve: Just what I was about to say.

Leo: Oh, good.

Steve: Is that my plan had been, for those listeners who actually do follow along, this was going to be the week when I would talk about Google's proposed new protocol to replace HTTP called SPDY, short for "speedy," and clearly they were trying to keep with the four-character HTTP feeling with SPDY. The problem is that - oh, and we talked about initiating TCP connections a couple weeks ago to get ready for this discussion because it's necessary to talk about the overhead associated with new TCP connections, where we talked about the way TCP figures out, from a packet-based approach, how much data it can send. So we talked about throttling, then, in anticipation of this.

The problem is, we also need to talk about HTTP, and there was just too much news this week. There is so much stuff for us to talk about, just pure security news, that we're going to, as we have a couple times, only a few times in the last seven-and-a-half years have we reverted to your original concept for this podcast, which was just some news.

Leo: Mega security updates.

Steve: Yeah. We've got updates and news and miscellanea and a great podcast of stuff, but we're not going to be able to get to the SPDY conversation which I had planned. That gets bumped into the second podcast...

Leo: Next year.

Steve: ...of 2012.

Leo: Yeah, because we've got questions next week. We've got sci-fi the week after. Then questions again.

Steve: Exactly.

Leo: Yeah, well, you're a busy fellow.

Steve: So that's our plan. Tons of stuff to talk about. Carrier IQ will not leave the news, and so you and I are going to enjoy, I'm sure, talking about that.

Leo: Good.

Steve: Lots of update stuff and other stuff. So we've just got what I'm calling the Mega Security News Update podcast, 331, today.

Leo: All right. Mega security updates. We had the Microsoft update, didn't we?

Steve: Yeah. And a gala event it is. We're a day after the second Tuesday of December. And we do seem to be maintaining this interesting sort of seesaw pattern of not much one month, a lot the following month, not much, and back and forth and back and forth and so forth. This is one of the big months. They're patching at least 19 different security vulnerabilities in Windows and other Microsoft products, that is, Office and Publisher are also represented. Three of these are critical.

And the good news is we finally got the long-awaited fix for that TrueType font rendering problem. I had been recommending that, because this didn't seem to have many side effects - I did get a couple reports of, I think, some PDF problems. But I was saying use that Microsoft quick fix button because this was being actively exploited by the Duqu trojan, taking advantage of a glitch in, unfortunately, in the kernel, giving malware access to whatever they wanted in the kernel because Microsoft had moved the graphics engine, GDI, into the kernel once upon a time for the sake of performance. And of course that was a huge mistake from a security standpoint. But that's the way things go.

So they fixed that, as well as another critical flaw in ActiveX handling and in Media Player. So three critical things are fixed. And then the rest, some 16 other vulnerabilities in Office and Publisher, just sort of generic, less critical, but important to do anyway. So that's our monthly Microsoft news.

I had a bit of a strange event with Java. Brian Krebs, who is of course keeping an eye on bad guys a lot, and I refer to him a couple times...

Leo: I hope he's doing well. You know he was the security guy at the Washington Post, and they - I guess they canned him. They stopped doing the column. And he's been doing his own On Security blog, and it's great. And I just hope - Brian, I hope you're doing well.

Steve: Yep. He tweets, and I do keep an eye on his Twitter feed because I get news there. And he does - he takes the time to really plow into topics. He seems to enjoy stalking the bad guys, stalking the stalkers, and, like, has, apparently from what he reports, he has personas that he has created out in that really dark underworld hacker community and is able to see what they're talking about. So his insights are unique in the industry and, yeah, makes him very valuable.

He referred to a new Java update, saying that it was Update #30. And we'd just finished talking about 29 and that it was important to do that because what 30 was ostensibly fixing was something that was being actively exploited in one of the more popular exploit kits called Blackhole. And of course, as soon as a vulnerability goes into an exploit kit, it's quickly rolled out, out into the real world, because kiddies who are not able to develop these things themselves use these exploit kits, much as it sounds like. They sort of wrap their own payload and use the exploits that are bundled into this kit in order to get them installed in machines. So this is unfortunately a predictable but dangerous consequence.

So I did what I had said to our listeners when we were talking about #29. I went to

Java.com, clicked on "Do I have Java installed," although I already knew that I did because there are some things that I use Java for. I mentioned GRC has a big number calculator now off of our Miscellaneous menu that I use for doing crypto calculations because it'll handle ridiculously large numbers of digits and so forth.

But when I went there, it said, oh, yes, you've got the latest, #29. And I thought, okay. Well, Brian is really always on the ball here. And he did say go to the Control Panel applet. And there is, on a Windows system, if you've got Java installed, in the Windows Control Panel there'll be a little Java thing. So I went there, fired that up, and it seemed to be happy. But then I manually told it go look, and it said, oh, we've got #30 for you. So...

Leo: That's weird.

Steve: ...maybe they - yeah. Maybe they just haven't gotten around to notifying their website. I hope they do that because people who are, I mean, their automatic update system isn't functioning automatically at this point, and this is an important thing. So if anyone's got Java - and again, I will remind everyone, don't get it if you don't have it because, I mean, if you don't know you need it, it is an actively exploited opportunity. If you have NoScript involved, you're probably safe because NoScript will block that unless you give sites permission. So if you're just bouncing around the Internet cavalierly, NoScript is your friend, or NotScripts over on the Google Chrome side. But you do have to go get this on purpose, at least at the time of this podcast recording. Hopefully, maybe somebody from Oracle is listening to this, and they'll go, whoops, we forgot to increment our count from 29 to 30.

Leo: Sometimes with, well, you know this, with updates they don't roll them out universally all at once because they don't want to kill the servers or whatever.

Steve: It was my thinking, too, yes. So we're expecting out-of-cycle patches next week. We're still waiting for Adobe to catch up with Reader and Acrobat. I think it was the version 9s, as we talked about this, I think, two weeks ago, probably you and me, Leo, because there was a zero-day flaw that was discovered in the PDF rendering that Reader and Acrobat both do which is being actively exploited.

The sandbox in the v10 technology does contain this. That is, it prevents it from being effective. The flaw is there, but it can't get out of the sandbox. Consequently, Adobe is not rushing to get that fixed. They are rushing to get the pre-sandbox versions of Reader and Acrobat updated, which they have promised, like I think I remember the 16th, which I think is, like, toward the end of next week? Or, no, no, that would be the week of the 16th. Wait a minute, no, maybe I'm thinking of 18th. In any event, it's on its way soon, but it hasn't happened yet. However, two new zero-day vulnerabilities have just been revealed in Adobe's Flash Player.

Leo: Prompting the query in our chatroom: Which is worse, Java or Flash?

Steve: Yeah, take your pick.

Leo: Yeah, no kidding.

Steve: So a Russian firm that does vulnerability research and sells their protection to customers is taking the position of, we're not telling Adobe because they don't pay us. So...

Leo: Oh. Oh, that sucks.

Steve: Well, you know, but they're selling their proprietary information to their customers. And it would make it less valuable if they provided it to Adobe because then Adobe would fix it, and then they wouldn't be offering exclusive protection to their customers. So it's a little, I agree, it's a little strange. But that's what they're doing.

They bypass both of these new, undisclosed, but proven and demonstrated in a video that they have, zero-day vulnerabilities; bypass both of Windows' anti-exploit features that we've talked about: DEP, which is the Data Execution Prevention, where regions of memory are marked as nonexecutable, like for example the stack, which normally only contains data, you don't typically execute the stack, and so that prevents stack overflow exploits, but not in this case; and ASLR, which is the Address Space Layout Randomization, which takes sort of the inherent modular nature of today's operating systems where different pieces are contained in separate modules, and Address Space Layout Randomization scrambles them all up so that different instances of the operating system are not always in predictable places. And that prevents the bad guys from being able to jump to known code and get their work done by sort of repurposing code in the operating system. If you don't know where it is, you can't jump to it reliably. But these vulnerabilities bypass all of that and work anyway. Oh, and they both escape from IE's sandbox. So the sandbox...

Leo: Whoa. Gee.

Steve: Yeah. So the sandboxing in IE is also ineffective.

Leo: Amazing.

Steve: Now, at the moment, this is Windows only. But they have promised soon to have a Mac OS X version.

Leo: Good. Because we want parity.

Steve: Because, exactly.

Leo: It's only fair.

Steve: Oh, goodness. So nobody knows what these are. The problem is that, as we know, you can often reverse-engineer patches in order to figure out what it was that was patched. And so the expectation is that the malware guys are going to jump on this and are probably in the

process of doing so. But there's nothing we can do about it. I mean, we users can only not use Flash in order to avoid the problem. So again, you want to be extra careful today about where you go and what links, especially what links you click in email, because anything that can invoke Flash which is malicious, if bad guys have figured out what these problems are that only this one company is selling their customers the fixes for, then that's a vector of exploitation. So Adobe has got lots of...

Leo: You got 'splaining to do.

Steve: Oh, yes, exactly. They're in the dog house. Now, speaking of dog house, we have Carrier IQ once again in the news. And I was the first...

Leo: Really, I thought we were done with this.

Steve: I had hoped we were done with it.

Leo: I thought while I was in Paris it would be all over.

Steve: Yes. But what happened was the FOIA, the Freedom of Information Act, was...

Leo: Oh, I saw this. This was interesting, yeah.

Steve: Yes. A request was provided to the FBI under the Freedom of Information Act last week, asking about the FBI's own use of Carrier IQ's technology. Now, it would have been nice if they'd said, "We don't use it." Instead, they said, "We're not saying."

Leo: Because...

Steve: Yes, they...

Leo: ...it would reveal information about ongoing investigations.

Steve: Yes. And in one place I saw the phrase "ongoing investigations." Elsewhere I saw them saying - officially they said that the release of such documents, quote, "could reasonably be expected to interfere with law enforcement proceedings."

Leo: Not good.

Steve: No. Now, okay. There are a couple possibilities. I don't want to - first of all, we'll be talking about this for the next few minutes, so there's a lot of interesting information here. There has been, as a consequence of the brouhaha over this, Al Franken, a Minnesota congressman - or senator.

Leo: Senator.

Steve: Senator Al Franken has launched a congressional inquiry into what's going on with this whole Carrier IQ business.

Leo: What's the deal?

Steve: So, yes. So there's a chance...

Leo: It's probably because Al Franken used to be on "Saturday Night Live," every time you say "Al Franken wants to know," I just get this comedic sense to it. But of course he's a senator. This is very serious.

Steve: And he's ended up really impressing people.

Leo: He has. He's been very good on privacy issues.

Steve: Yup. He's been our friend. So there is a chance that the FBI's response does not involve their use themselves of Carrier IQ, but rather that they're involved in the congressional inquiry, that is, Congress has said to the FBI, please look into this. So I don't want to, like, send off any wolf-crying false alarms here. This might just be that they're the agency that Congress is using, as they would, to inquire into what's going on with Carrier IQ. So this FOIA request is being denied on the basis that it's the inquiry that they can't talk about rather than their own, you know, they've been rubbing their hands together, having fun with Carrier IQ behind the scenes without us knowing about it.

Leo: "Did you see that text she sent? Heh heh heh." Yeah.

Steve: Yeah. So, also, Carrier IQ is stating that, while they collect the data, they do not own the data.

Leo: Oh. Who owns it?

Steve: It is provided to the carriers, so any requests would need to be made to the carriers, not to them. And they do, however, maintain servers on behalf of the carriers. But contractually they're contracted to be the data collector, but they are not the data's owner.

Leo: They're just following orders.

Steve: Yeah, exactly. Now, here's the problem. Provisions of the U.S. Patriot Act would prevent Carrier IQ's disclosure and would indemnify them, Carrier IQ, against nondisclosure. So they could - this is also what they would be saying, and protected by the Patriot Act, if they were a source of data and been told you can't say anything about it.

Leo: So the scenario is, if I read between the lines - and we've always thought maybe the NSA was using Echelon. That was the name used for this presumed technology. The British intelligence admitted it, MI5 admitted that they use Echelon to scan electronic transmissions for keywords like "bomb" and so forth. But there's...

Steve: I wish you hadn't just said that, Leo.

Leo: There's a gaping hole because, if I say "bomb" in a podcast or on my text messaging, they can't find that.

Steve: Now Elaine is going to transcribe it, and it's going to be on my website.

Leo: Hard to believe we can't...

Steve: And before you know it, it'll be what happened to Gibson?

Leo: Yeah, yeah, yeah. By the way, they don't have to invoke the Patriot Act. One of the features of the Patriot Act is you don't talk about the Patriot Act. You don't have to ever...

Steve: No, exactly. And that's my point, is that they could deny that they have anything going on.

Leo: They're indemnified, is the point. They can't be sued.

Steve: Exactly.

Leo: Yeah. They can't be sued.

Steve: Okay. Now, on the 12th, which was two days ago, as part of Carrier IQ's response to all this, they produced a 19-page document. I tweeted the URL of that earlier today. So anybody who is interested can, if you're not following me, that's fine. Oh, and by the way, I don't know if you know, but I crossed a milestone, 25,000 followers.

Leo: That's great, Steve.

Steve: Tom and I talked about that, I think, last week. So, yeah.

Leo: Yeah. And you don't have to follow Steve to see what he says. You can just go to Twitter.com/SGgrc.

Steve: Exactly.

Leo: And you see all his tweets.

Steve: Exactly.

Leo: But follow him, and that way you'll get him in the Twitter stream.

Steve: Well, unless you're not - unless you're Jerry Pournelle, and you just...

Leo: You don't care.

Steve: You're not going to be a Twitter tweeting person.

Leo: Does he not - does he still - 'cause I maybe he'd change his tune on that.

Steve: I don't know what happened. I do think I remember that he was going to give it a try.

Leo: Yeah. He's pretty "with it."

Steve: So their 19-page document is interesting. So some things that I discovered by reading it, as I have, is that they - whereas their first reaction to Trevor Eckhart's discovery, and he was the person who we talked about who showed the phones capturing keystrokes and logging - it was an HTC Android device - was logging all of this scary stuff. Their first reaction, of course, was to issue him a cease-and-desist order, threatening legal action.

Leo: Kind of a mistake.

Steve: Now they're thanking him.

Leo: Yeah.

Steve: In the PDF. Thank you so much for discovering debugging code that was left in by mistake.

Leo: Oh. Oh, it's debugging code.

Steve: Yeah. We never - we meant to turn that switch off.

Leo: Oh.

Steve: And we fell asleep at the switch.

Leo: Sure.

Steve: So, I believe it, though.

Leo: It's the kind of thing you would log in a debugging situation.

Steve: Yes. And Trevor wasn't able to show that it was ever being sent. It's disturbing that a plaintext log file in an Android device is capturing all that. You really don't want all of that being captured in a plaintext log file sitting there in your phone.

Leo: We spend so much effort using LastPass to encrypt our passwords and stuff, and it would just save me so much trouble to know there's, well, there's a plaintext file with all my passwords right there. I could just open that up, and I'd see everything.

Steve: Yeah. Now, okay. You could also take the - you could argue that, remember, that, well, the ISP gets it all anyway. That is...

Leo: But do they in SSL? No, they don't with SSL.

Steve: Yeah, see, you're following me exactly, Leo. That's exactly where I was going with this was that, yes, SMS messages and unencrypted, well, and URLs that are for pages we're pulling, they would be able to see those things. But exactly as you say, anytime you're tunneling, they can't see into your tunnel. So they, then, are only carrying opaque traffic. So if you use a VPN, or if you're inside of an SSL encryption, poking around doing things, that's opaque to them unless they're grabbing things before it gets encrypted. And that is what being on the device uniquely allows them to do.

Okay. But what they're explaining in this 19-page document with lots of screenshots and, I mean, it's nicely written - I wish it didn't start out, I wish the title of the document was not "PR.20111212."

Leo: [Laughing] Spin.doc.

Steve: [Laughing] Exactly.

Leo: Wow.

Steve: I know. So it's like, okay, do you have to call it public relations? Could we not - how about TechDetails.doc.

Leo: Excuses.doc.

Steve: Oh, goodness. Anyway, so this thing, what we now know from reading this is that there's three different ways that this stuff, this Carrier IQ thing, can be put on your phone. It can be sort of stuck on before you get it. It can be added by the user and therefore removable after you get it. Or it can be, quote/unquote, "embedded," which gives it much greater reach. That is, if it's sort of stuck on - they had a term for it I don't remember now.

But it's like the first way they talk about it being added is sort of casually added by the phone's provider, but not deeply embedded. And, if so, it doesn't have access to much. Like it can't - it only has access to what a typical application would have, and you don't get things like RF signal strength and tower location and those sorts of things that you get if you're in the embedded mode. So looking at the embedded mode, it's got access to all the information that the carrier, the service provider, would like to have.

So the way this thing works is it's driven by profiles. Profiles determine - and it's like a config file, essentially - what data is collected, how often it's collected, how long it is saved, and how often it is uploaded to the carrier. The typical use of this, okay, and this is what they're now, in their PR document, they're acknowledging, 200K of data per day per device.

Leo: Whoa.

Steve: So, yeah. So old school people say, 200K? Well, I mean, we've seen what I can do in 200K. But still, that's a lot of data. So typically, every 24 hours, during a time when the device is not in use, the Carrier IQ-accrued data is dumped up to their servers and/or directly to the service provider. Profiles are also downloadable on the fly. So the nature of the data which they're collecting can be changed. Now, this document makes it very clear that never, ever, ever have SMS messages been collected. And that was one of the things that concerned people. On the other hand, SMS messages always go through the carrier.

Leo: The carrier's always been able to see those.

Steve: Yes.

Leo: And I know for a fact that you can subpoena those. So any text message that's sent in the clear is stored by the carrier and can be retrieved by the carrier upon request.

Steve: Right, so...

Leo: We've known that.

Steve: So what they acknowledge they are collecting are all the phone numbers dialed, the URLs visited, and detailed location and time. So if the FBI hasn't already discovered this honeypot of information, they certainly know about it now.

Leo: Well, but again, all of that information would be also available to the carrier. Maybe not URL. Well, yeah, URLs, too, because they're the ISP as well as the carrier. So they've got text messages. They've got phone numbers. You see the phone numbers on your bill.

Steve: Well, what we have - what wasn't clear to me, what isn't clear to me is what sort of granularity of location data the carrier is storing. And it's now clear that the Carrier IQ app is providing extremely granular, or can provide extremely granular information. So a scenario, just to walk us through - we don't know this is being done. But using the Patriot Act, the FBI could compel Carrier IQ to download an enhanced spying and tracking profile to any phones of individuals whom they wish more information on. And the Patriot Act allows Carrier IQ to do that, the FBI to essentially crank up the resolution of tracking to maximum, which gives them extremely granular location and positioning and activity information on individuals which may well be in excess of what the carrier would normally aggregate.

Carrier IQ makes the point defensively in this document of saying, we don't want SMS messages. We don't want - there is so much data coming and going through these phones that our job has been to condense the information, to distill it to only what the carriers are asking us to capture for them. And I believe that. I mean, if I were an engineer, if someone said, "This is how we want the system to work," the first thing you want to do is minimize the bandwidth that you're consuming and storing on these devices. So to me that makes sense. But it also really does - it really is the case that this technology allows our devices to be tracked. But your point, also, Leo, is carriers certainly have that capability themselves.

Leo: Sure. Sure.

Steve: They know which cell towers you're at relative to where you are. And your phone also, if it's got WiFi, and it's logging itself into hotspots whose locations have been logged with the whole - all of the several different hotspot tracking services that we know exist, then that's there, too.

So anyway, we understand more about what this is. I do believe that Trevor stumbled on debugging code. I mean, it makes sense that that's the case. Carrier IQ has formally stated that that's the case, and it makes sense. So they are a technology which we are now aware is in our phones. They give a couple examples of how, for example, a carrier would use this technology. If you call them, you call your provider, AT&T for example, and say, hey, why is my battery draining in three hours now, it never used to do that...

Leo: Let us check our logs.

Steve: Yeah. No, truly. They're able to say, on such and such a date, you installed ABCXYZ app, and it's responsible for what your battery is doing. The technology now allows them to do that. Or they're able to say, oh, yeah. If you say, hey, why am I always dropping calls between Exit 34 and 35 on the 97, and they'll say, oh, yeah, we are aware of that. There's an outage area there, low service availability. We're in the process of building some more towers, so make sure you don't hit one when you're driving on the freeway. So...

Leo: They say that, really?

Steve: So anyway, that's what's going on. They have, they really do have a technology in there. I'm convinced primarily it's there to help them with tech support. And as you said, Leo, correctly, they don't need this in order to provide location tracking and where was So-and-so at such-and-such a time.

Leo: In fact, that's a fairly controversial issue because law enforcement currently doesn't need a search warrant to ask for that information. They can do something called a "pen register." And in fact apparently all the carriers have portals for law enforcement where they pay a couple of dollars, and they could find out where anyone was at any given time.

Steve: Wow.

Leo: Because that's really what you're carrying around, by the way, is a GPS device that's always broadcasting back to the carrier where you are.

Steve: It's tracking. If it's on, it's tracking.

Leo: You ever watch "The Bourne Identity"? What's the first thing Jason Bourne does when the scared woman gets in the car with him, and she's running away from the bad guys? He takes her phone and throws it out the window.

Steve: Throws it out the window.

Leo: Well, guess why? Okay. Sorry.

Steve: Yeah. I want to mention, because we'll come back to the topic of the DMCA a little bit later, but had the DMCA - had this involved crypto, then what Trevor was doing would have been criminal. And...

Leo: Oh, not protected as - isn't it protected as research, though? Like Ed Felten and people like that, aren't they protected? In fact, wasn't that his response?

Steve: I thought that, as I understand it, the DMCA criminalizes research.

Leo: Oh.

Steve: That was the problem, is that it's preventing researchers from talking about the crypto of commercial products because they have to breach the DMCA in order to do the research. Which is really distressing. I mean, that's my big problem with the DMCA is it doesn't allow security researchers to plow into stuff.

Leo: Oh, that's not good.

Steve: Without becoming criminals. So, and I would argue that all of this, what's come to light with Carrier IQ, is really good. I want Al Franken to ask, to get somebody to look into this to verify and to shine a bright light on this because this really should not have been kept as quiet as it was. Even if they're not doing anything wrong, even if in the fine print it says this is what we're going to be doing, people still don't know about it. And we need to know about it. Benign as it is, it would just be nice to know this is what's going on.

Leo: I always feel that what protects us is that the massive amounts of data that these kinds of things would collect, the 200K about each and every one of us each and every day, renders it pretty much useless for kind of casual spying.

Steve: Although - yes. Although what I hear people say sort of in general, when they're not worried about security, is, well, no one cares about me.

Leo: Right.

Steve: It's like, okay, well, today.

Leo: And we do know the technologies, computer technologies allow people to go through, sift through that kind of data, looking for patterns and...

Steve: Determine who they should care about.

Leo: Right. So this is - it's interesting because there is a tradition in our legal system that law enforcement is not allowed to go on what they call "fishing expeditions," that they have to be investigating a specific crime, and they can't just look at your stuff to see if you're doing something wrong. That's not allowed. And that's exactly how this kind of data could be used. And of course I can understand law enforcement saying, "But it would be so useful if we could just get a database of everything everybody does online and sift it for bad behavior. Think how useful that would be." But that's not allowed. That is specifically prohibited by our Constitution, thank goodness. All right.

Steve: Well...

Leo: Well, there you have it.

Steve: You want to go to a site called YouHaveDownloaded.com.

Leo: [Laughing] You know, actually I do want to do this because I want to see if anybody in my office is using BitTorrent.

Steve: YouHaveDownloaded.com is a new service which anyone can go to. And it looks at your connection IP and cross-references a database it is continually building of all the IPs they're aware of which have been used for downloading torrented files and what files have been downloaded. Apparently people who are active torrent users go to YouHaveDownloaded.com and see a listing of their entire library.

Leo: Amazing. No one here is downloading anything from BitTorrent. Thank goodness.

Steve: That's good news, yes.

Leo: But you know who has? Sony. Busted.

Steve: Yup. Now, one thing I noted is that they're not establishing an SSL connection. They support SSL for their domain, and you can go to https://youhavedownloaded.com. The reason that's significant, for example, is that I had to do that with ShieldsUP! in order to more reliably get the user's IP because anybody, for example, with a Cox Cable modem, if they use a non-SSL connection, the IP is Cox's IP, not theirs.

Leo: Ah.

Steve: Because you go through Cox's caching proxy on the way out to the Internet for - which does a number of things that helps users because it's caching, so you get answers back quicker from Cox than you would out from the Internet, and it also reduces the bandwidth that Cox needs to pull from the Internet. But it means that you don't have the right IP. Now, it is possible to disambiguate that somewhat because proxies are supposed to add a header saying that they are forwarding this request for a different IP. So maybe these guys have done that, and I would hope so. Otherwise it could be the case that you'd be getting false positives and seeing other people's torrents being attributed to you, which would not be good.

Leo: Well, they do say this site is just for show, that it's a demonstration and shouldn't be used as for incriminating evidence.

Steve: And they're opening - well, and I think it's a little bit of a wakeup call, also. They said...

Leo: Yeah, well, every - the truth is, though, and I've said this for years, and nobody ever pays attention, but BitTorrent has never been designed to be private. When you're exchanging files with people, I can see your IP. I can see who's seeding by IP address. It's always been that way.

Steve: Yup. So they said, "This means that you are using...." Oh, so when I went there, they said, "We have no records on you." And they said, "This means you are using a private torrent tracker or, of course, you may not be a torrent user at all," as happens in my case. I'm just not a torrent guy. And they said, "It happens. Please entertain yourself. Feel free to see what other people have downloaded. The search box is on the top. If you have any friends who use torrents, use it to scare them off. We also have a widget that you can install in your website, blog, or Facebook page. Or you can just send them a link to this site. They will see a table similar to what you see below. The only difference - they will see their downloads."

So anyway, I tweeted this earlier, and a lot of people responded that, whew, I'm clear. Also some said, hey, but IPs are dynamic. And it's like, well, yes, they are. But they don't change all the time.

Leo: Well, and this site says we record timestamps. So we know exactly which IP was using it when.

Steve: Exactly. And so, if they were - if they had to comply to a subpoena turning over their records, then that could be cross-referenced with ISPs that do maintain a log of who has which IP when. And, for example, Sue, my office manager/bookkeeper, is using a cable modem with a router, which means that her IP, her public IP is relatively static. I know when she changes it because she needs me to update that information because we use her IP as one of a multilayer security measure for her access to some content on our servers. So I know when I change it. And I don't change it more than once every couple years. That's how sticky these things are, unless you're deliberately disconnecting from your cable modem or your DSL for a long time. If you stay off of it for a long time, then there's a chance somebody else will get that IP allocated to them, and you'll get a different one when you reconnect. And in fact that's what happens. Like if they shut themselves down when they're going on vacation, when Sue and her family comes back, their IP will have changed when they turn things back on again. But in the normal case, it's not changing. Those DHCP leases are being renewed, and you deliberately get the same IP you had last time. So they're more static than most people think.

Leo: So, now, somebody in the chatroom's saying, oh, this is a joke. The site's a joke. It's not - is it a joke? No.

Steve: No.

Leo: It's real. There's limits to what you could do with this. And the reason they created this is to point out that, unless you're doing something to protect yourself, you are publicly sharing these files.

Steve: Correct. And I know for a fact that there are people who are public torrent users that this site knows about. So it's certainly not a joke.

Leo: Yeah, I mean, they say at the bottom don't take it seriously. That doesn't mean it's a joke. It's a...

Steve: I think what they're trying to say is, it is not the case that, if we don't have you, nobody does.

Leo: Right.

Steve: Because they're tracking a bunch of trackers, but they're not trying to be the MPAA or the RIAA. And so no one should believe that, if this site does not - if you are a torrent user, and you have downloaded things in the past, yet you come off clean here, that doesn't mean there aren't records of prior activity somewhere.

Leo: Right. It's a joke only in the sense that they're not going to do anything with it. But I think this is actually a good public service.

Steve: That's exactly how I feel. It's a wakeup call. It's useful.

Leo: I mean, I've known this. But maybe not everybody does.

Steve: Exactly. Speaking of public services, Facebook has added themselves to the elite list of companies who pay security researchers to find bugs. And in fact Brian Krebs's posting calls it "Bugs Money." But get this. The way Facebook is paying is unique. When a researcher, the first time a white hat researcher finds a bug, they send them a Visa debit card. Cool-looking card. It's custom-made for Facebook. And on this Visa debit card it says "White Hat," in large print, "Bug Bounty Program." So you receive money on this Visa debit card. And if you find more bugs with Facebook, they simply transfer more money onto your card. And they have a page that I hadn't known about before, but Brian linked to it. It's Facebook.com/whitehat. And that is a listing of all the names of researchers who have identified problems in the past with Facebook.

So anyway, I salute Facebook for doing this. This is a good thing. I'm glad that they are, I mean, this makes sense. It makes sense to incentivize developers, security researchers, to find problems because we know how difficult it is to have none. And certainly Facebook has had its share of lumps in the past.

Also in the news this week, Microsoft has put into beta the offline version of Windows Defender, available for download both in 32- and 64-bit versions. I would imagine you could Google it. I just tweeted the news. So anybody who wants to find it can. Just as you said, Leo, look at Twitter.com/SGgrc and pick up the link to it. This is installable on CD, DVD, or USB. And the advantage is this is probably THE way to deal with rootkit-style problems, that is, especially boot sector rootkits which are compromising Windows before it boots up.

So by using a preboot CD, which now Microsoft is providing, it's possible to boot the CD or the USB rather than the OS, never letting that boot sector, the OS boot sector execute and allow a rootkit then to start subverting the OS before any of the OS-based antimalware technology has a chance to come online. So of course it's free, and you can choose a 32- or a 64-bit version, depending upon what OS you're running. And so that would - wait, wait. OS or chipset?

Leo: OS. Almost certainly. Yeah, it says 32- or 64-bit version of Windows.

Steve: Yeah, but why?

Leo: Oh, that's true with all software. Often.

Steve: No, but remember - I know. But this is booting on the chip, not the operating system.

Leo: Oh. Oh. Well, perhaps the installer, then. I don't think they - they care about the installer.

Steve: Ah, I'll bet that's exactly right, Leo. Yup, I'll bet you're right.

Leo: Yup. Although why not just do it all at 32-bit, I don't know.

Steve: It would be agnostic to which version of Windows you run.

Leo: Right.

Steve: So, SANS Institute newsletter contained a little blurb that I had not seen anywhere else, but I was glad for it. And this is the news that Lamar Smith, who's a Texas U.S. Representative, has introduced some changes to the oh-so-controversial Stop Online Piracy Act, SOPA, which attempt in this case to temper the proposed legislation's reach, which could only be good. SANS wrote that, "Originally, SOPA allowed rights holders to have payment processors cease doing business with suspect websites without a judge's approval." Now, that was very worrisome, meaning that...

Leo: Yeah. No due process is that that means. That's terrible.

Steve: Precisely. And it cuts off your revenue flow. So it's like, okay, payment processors are just going to stop accepting credit processing from your site. It's like, oh, crap. Now, however, before a site could be taken down, the rights holders must obtain an order from a judge that will - okay, "now" meaning pursuant to this revised legislation, if it happened - the rights holders must obtain an order from a judge - wait, no no no, I'm sorry. I got this wrong. So the original legislation was proposing that, with no judge's involvement, an alleged aggrieved...

Leo: It was the Chanel - was it the Chanel handbag story?

Steve: Yeah, that somebody who believed their rights were being violated could have payment processors cease doing business.

Leo: Oh, okay.

Steve: And it says, "Now, before a site could be taken down, the rights holders must obtain an order from a judge to get payment processors to sever business dealings with a suspect site," which is the way it ought to be.

Leo: Of course, yes.

Steve: Now, what I don't understand is it says, "The legislation will not apply to sites that end with .com, .net, and .org.

Leo: Oh, you mean the Internet. Oh, no, it doesn't apply to that.

Steve: Yeah. It says, "Only foreign websites will be subject to SOPA's provisions." So that also sounds good. If I read this correctly, the other change is that .com, .net, and .org are being excluded from SOPA.

Leo: I don't think that, well, those are the changes.

[Talking simultaneously]

Leo: Oh, you know why? I get it. They're going after these pirate sites, is what they're trying to do, .cn or...

Steve: Yes.

Leo: ...you know, those French, and not the...

Steve: Careful there, Leo. You spent the last couple weeks over there.

Leo: I just might point out that, Pirate Bay? Dot org.

Steve: Uh, yeah, good point.

Leo: I mean, anybody can be a .org, .com; right?

Steve: Yeah.

Leo: There's no, like, well, you have to be - you have to license it. No, anybody - so this is stupid. If that's really what they want to do, that's good. That's completely...

Steve: To defang SOPA.

Leo: Defangs it, yeah.

Steve: Yeah.

[Talking simultaneously]

Leo: They're showing, again, their complete ignorance of everything that we hold sacred.

Steve: Yeah. It says, "Remaining untouched are provisions that allow the DOJ [the U.S. Department of Justice] to demand that Internet service providers block customers from visiting these sites."

Leo: Oh, that's so the - so the ICE takedowns; right?

Steve: Right. "The bill no longer requires ISPs to alter DNS, but they may still choose to do so to comply with blocking orders."

Leo: Look, the whole thing is just a bad idea. Just...

Steve: I really would say the whole thing seems, now, it's gotten byzantine.

Leo: Yeah.

Steve: It's so bizarrely complex.

Leo: Dumb.

Steve: Okay. Now, news on my front. I have switched, as I said I was going to at the end of the year, from VeriSign to DigiCert.

Leo: Good man. I guess.

Steve: I had my GRC - I had three certificates. I had GRC.com, www.grc.com, and www.grctech.com. I use that in order to deliberately create a third-party for my third-party cooking - cooking - cookie system.

Leo: Well, you have to cook cookies. They're raw. That's not good for you.

Steve: That's that third-party cooking you've got to watch out for. So I could not be happier. It was a perfect, painless switch. And I'm super pleased with DigiCert. Also, I have what I always wanted, Leo: not just a change, but I am now EV. I have GRC is...

Leo: Oh, good.

Steve: Is Extended Validation.

Leo: Oh, excellent.

Steve: And what is very cool is that I got the EV cert for just the root domain, GRC.com, and "www" was included. So whereas VeriSign/Symantec - actually it is now Symantec, but they're still using the VeriSign - I think they're still using the VeriSign domain. Whereas they would have charged me $1500 for each, I paid something like $500 for both. And I still have two more slots available, meaning that if I wanted mail.grc.com or two other somethings.grc.com, I can myself, just using the web panel, because GRC.com has been verified, I have up to three different subdomains, one of which is www, but I've got two others that I can allocate anytime I want to.

And they allow this to be installed on multiple servers, which, for example, VeriSign doesn't. And I can even use different private and public keys. So I could have a different server generate a CSR, a Certificate Signing Request. I submit that through a web form. And with zero delay, because this is being issued to the same domain, which has already been verified, they will issue me new certs for another server with separate keys.

Leo: That's great.

Steve: So not having to reuse the same keys, which of course is a security concern if you spread your keys around too much, here they're - and you can do it as much as you want to. Anyway, I am completely bullish. But...

Leo: But...

Steve: Something bad happened.

Leo: Oh, dear.

Steve: We installed the certs, I installed the certs, on Friday. And we took a hit in revenue. We had the - SpinRite sales collapsed.

Leo: Oh, dear.

Steve: With the lowest revenue ever, we've ever had, on Sunday.

Leo: What the hay?

Steve: Well, and so I was checking the server, and nobody was buying SpinRite. All of a sudden.

Leo: Uh-oh.

Steve: And but we weren't rejecting sales, there just weren't any. And then I had a thought. What if a high percentage of the people who buy SpinRite listen to this podcast?

Leo: Yes? Yes.

Steve: And they've installed Certificate Patrol in Firefox, as I have encouraged everyone to do. The scariest warning that Certificate Patrol can give you is that the vendor of your certificate has changed. That is, the apparent vendor has changed. Because that would be, I mean, that is the hack. If somebody was performing a man-in-the-middle attack or got your certificate fraudulently issued by some other Certificate Authority, then, I mean, this thing comes up with flashing neon lights and colored red. And I thought, oh, my goodness.

Leo: You scared everybody off.

Steve: I scared everybody off with a valid change.

Leo: Oh, boy.

Steve: And so finally, by, like, the end of, maybe it was Monday, I thought, you know, maybe that's what's happened. So I put, on the page where people go to buy SpinRite, a special new banner which celebrates our increased security. It's got the DigiCert EV seal up there, which you can only display, because it comes from them, if it's all true. And I explained, hey, we've got even more security than ever. And, oh, by the way, if you're getting any kind of scary notification...

Leo: That's good.

Steve: ...that's because we really did - yeah, that's good. That's a good thing because we really did go, we left VeriSign behind us - and happily so - and I couldn't be more happy with DigiCert. So please forgive us for scaring you. But then something else happened a couple hours ago, Leo. Dr. Mom sent me email.

Leo: Uh-oh.

Steve: And we know her. She's - you're referring to her all the time. She's an active participant with many of your podcasts. She said - this is her email I'm reading - "Thought you could use a good laugh." Well, I'm not laughing. Anyway, she said, "The, ahem, 'IT' department of our esteemed institution" - who I'm not naming - "has officially declared the GRC website 'Restricted under Internet Usage Policy because of potential security risks or inappropriate content.'" She said, "Probably they don't want us to figure out how lame their password policy is, nor that if you use ShieldsUP! on the system all the ports are wide open and exposed. Just thought you'd like to know that your website is now classed with .xxx and other sketchy places on the Internet. LOL."

Leo: That's frustrating.

Steve: Well, what I'm thinking, Leo, is that we may have upset some carrier, like who knows, some provider of border equipment that Dr. Mom's organization may be using. And I don't mean to mention Astaro. I don't mean Astaro. But that kind of...

Leo: No, but, yeah, or a MAPS or ORBS site, those kinds of thing, yeah.

Steve: Something may have - something somewhere may have noticed that our SSL certificate provider changed, and we're now subject to a false positive security alert, which Dr. Mom's organization subscribes to, or her networking equipment or IT department subscribes to, which is causing them to blacklist us. And that may be what's happened, is unfortunately the point, the lesson here is that, because, I mean, how much time have we been talking about or how much time have we spent talking about all the things that can go wrong with the whole PKI (Public Key Infrastructure) and SSL and Certificate Authorities and breaches and all of this. So maybe what's happened is there are now organizations which are assuming that anytime any company changes its SSL provider, warning flags go up. And of course I'm unhappy because we know this is a false positive. We're more secure than we were before, and I could not be more happy that I made the change.

But I'll bet you - anyway, I wrote back to Dr. Mom, under her real name, and said, uh, whoops. Maybe - I'm hoping that she will pursue this with her quote/unquote "IT department" and find out what it is, where this came from, because that would allow me to pursue it and figure out if somebody is giving us a false positive.

So anyway, really interesting. I don't want in any way to put anybody off of switching to DigiCert. Believe me, I'm not going back because I'm already here, and I'm really glad I'm here. I have control like I've never had before. I'm saving a ton of money. I've got EV certs, and I'm not paying $3,000 a year for them, I'm paying $200 and something because they're including other subdomains which are really important to me. I want to be able to have people use SSL, both for GRC.com and www.grc.com. Why should I pay double for that?

Leo: Yes. Right on.

Steve: So this is just very cool. And so I do recommend that for you, also. Oh, and Leo, I have to say also, I've just made a note here, the dumbest marketing promotion I've ever seen. Well, okay, "ever" is a long time. Symantec is now offering free 30-day trial SSL certificates.

Leo: [Laughing]

Steve: It's like, what? What?

Leo: Hey, hackers. Get your free certificate here.

Steve: How does that make any sense at all? I mean, first of all, no one who understands what they're doing is going to think that a free trial certificate makes any sense. What, you're saving a month? Is that the idea?

Leo: Yeah. Every month you can get a new one.

Steve: Oh, I'm sure they won't let that happen. And so, first of all, no one is more expensive than VeriSign. And only people who use VeriSign are going to be big guys. I mean, I've been there until now. I'm just not willing to pay that money for the benefit of extended validation. I want extended validation, but not at VeriSign's prices. So, but IBM and, I mean, I don't know who uses VeriSign. But someone certainly does.

Leo: People like IBM. That makes sense, yeah.

Steve: Yeah, because Symantec bought them, so they must have a good certificate-issuing revenue flow, and Symantec probably paid a hefty price for it. But the notion that I'm going to be swayed to spend money I don't have to because I can get a free 30-day trial, I mean, it's a pain in the butt to go through getting a certificate.

Leo: It is pretty funny.

Steve: You've got to convince your server to give you a certificate signing request. You go through all of this, people standing by the phones when they call you to make sure that you're there, and email loops and everything, and they check your whois and your Dun & Bradstreet and, I mean, it's a - you've got - it takes something to do this. And so it's like, whoa, yeah, gee. I mean, clearly you're not going to abandon it after 30 days, so maybe they think they're going to hook you this way. But anybody who used VeriSign would shop around a little bit. And, wow, I don't know. That just - I can't imagine anybody's going to take them up on that. Except maybe to get 30 days free.

Leo: Yeah. Well, maybe you do that before - you know you're going to sign up for a year. What is the minimum normal term? A year?

Steve: Three years you can get for non-EV, and that's the maximum. So normally I'm jumping through these hoops only once every three years. Or two years is the maximum for extended validation certificates, just because they want to tighten that up.

Leo: And you probably can't get less than a year.

Steve: No. I don't, I mean, you could stop...

Leo: Unless you get this special offer.

Steve: Yeah.

Leo: I mean, for - well, maybe - somebody said it's a Christmas holiday shop, and they only need a month.

Steve: Okay. There's a company called StartSSL.com or StartCom.

Leo: Yeah, yeah, I know them.

Steve: They give you a free certificate for a year.

Leo: Right, right.

Steve: So it's like, if that's what you want, just go there. And they're recognized by all their...

Leo: They won't do EV, though.

Steve: Not for free, but very inexpensively. They do offer EV. And they are a - they're in all the browsers. So they're also widely recognized. So it's like, well, that's...

Leo: Why did you not go to them instead of DigiCert?

Steve: Well, because that seemed a little low end, a little low...

Leo: You can afford...

Steve: I don't know...

Leo: You can afford a hundred bucks. How much is it? How much is it?

Steve: It is like that. It's not expensive for StartCom. I think it's maybe 150 or something.

Leo: That's good.

Steve: It wasn't much. So, yeah.

Leo: So everybody should have SSL.

Steve: Eh, well, maybe someday. Anyway, DigiCert is my company. I'm happy. It'll be nice if we can solve the mystery. Maybe Dr. Mom will get back to me and say, okay, here's the story. Here's why GRC got blacklisted. Because something happened. We're not recovered yet. So somehow there was a side effect. And it wasn't that I went to DigiCert. I really want to make sure people don't get the wrong impression. It's that I changed. And change should not be a bad thing when it's an improvement. And this was definitely an improvement. So we'll see.

Okay. OAuth. I got email from someone who asked me if OAuth had a bug because he - let me think what this was. He went to a site where he wanted to authenticate himself with Twitter. And this was a bad site that he went to, and his profile changed, and they began sending out tweets on their behalf.

Leo: So he got hacked.

Steve: And he said, so - well, no. He actually didn't. And he said, doesn't this mean that Open Authentication is broken or buggy or something? And I said, no, it means that Twitter gave the requester rights to change your profile, believe it or not. Which boggles my mind.

Leo: Well, here's how I would guess the scenario went. He thought it was OAuth. It looked like OAuth. It may be they made a page that looked, because with OAuth you're go back to Twitter, that looked just like Twitter. But instead it was a fake site that wasn't Twitter, and he gave them his credentials, thinking he was logging into Twitter. So there is a - there's a potential hole in OAuth.

So I go to a site, right, and it's pretending to be OAuth. Well, how does OAuth work? When you go to the site, it says, okay, we're going to log - you've got to go to Twitter to log in, and they'll send us a token back. So what if I'm a bad guy? I'll say the same thing. I'm going to send you to Twitter now so we can OAuth you. But instead of actually sending you to Twitter, I send you to Hacker.

Steve: Twitter.ru.

Leo: Yeah. And I make a page, looks just like a Twitter OAuth login, and you give it your login and your password. You say okay, and it pretends it's sending a token back to the hacker. But meanwhile they've got your credentials. There was no OAuth transaction. I suspect that's what happened.

Steve: You exactly laid out a beautiful hack for OAuth, which reminds our listeners that, when you're doing this, you absolutely need to make sure that you are where you think you are.

Leo: It's not always easy because sometimes this happens on mobile platforms, right, on your phones. And you may not - the address bar a lot of times on phone browsers, because of limited screen real estate, is not visible.

Steve: Oh, in fact, I find myself doing that with Safari. I was somewhere I wanted - just the other day I wanted to make sure that I was - because I was at Starbucks, and I wanted to make sure that what I was doing was in an SSL tunnel. And it was - I had to, like, look all over the place. And finally I found a little padlock on the tab. And it's like, oh, there it is, okay.

Leo: People are fairly easy to fool.

Steve: Except that...

Leo: Not our listeners, but...

Steve: Except that this was not the scenario...

Leo: Oh.

Steve: ...that actually occurred. But I'm glad you went through that because you're absolutely right to remind our listeners this is a problem. I was logging into bitly the other day, and I had not been for a long time. Was that it? Oh, no. I created a new - I know what it was. I created a new Twitter account that I am going to get around to telling everyone about. It's called SGreads, is a new stream for me.

Leo: Ooh, I like this. Is this Twitter.com/SGreads?

Steve: Yes.

Leo: I love that.

Steve: And because for some time I've been running across things in the morning, during my morning time at Starbucks. I end up finding good stuff sometimes, and just on whatever topic it happens to be. And I thought, you know, I ought to create a stream of those. So people don't have to get them if they don't want them. But if they're interested in reading things that I think that sort of generic people would be interested in, there's a way to get that. So...

Leo: And that is - by the way, you're getting very close to being a blogger. Because that's really what a blog originally was. Om Malik, who's gone back to doing that, every weekend he does a "Here's what Om is reading" blog post. And that's exactly kind of what the original idea was for blogging. So, Steve, you're reinventing the Internet step by step.

Steve: Well, so what happened was, I went to bitly, and I wanted to tell it about this new account.

Leo: So it can keep the stats, of course, yeah.

Steve: Yes. So that I could use link shortening for, like, long URLs with this SGreads account. And so it needed me to authenticate that I owned that account with Twitter.

Leo: Right.

Steve: So bitly used OAuth and took me to Twitter.

Leo: Okay.

Steve: Here are the rights that bitly was given: Read tweets from my timeline. Okay, everybody can do that. See who I follow, and follow new people. So...

Leo: Ooh, I don't like that. But I know why they did that.

Steve: I don't like it either, and you can tell me why in a minute.

Leo: Okay.

Steve: Update my profile.

Leo: Not good.

Steve: And post tweets. Well, they only need to post tweets. As far as I can tell, the only thing bitly needs to do is post tweets. Now, it says bitly will not be able to access my direct messages or see my Twitter password. Well, that's the whole reason we're doing this.

Leo: So the reason I think it was allowing you - you were giving permission to follow is this happens all the time on a site. It says, as part of this, and would you like to follow bitly? And you say yes. And then they can do that one thing. But they...

Steve: Ah.

Leo: I think that's not - for that one purpose, to do that is not okay.

Steve: And update my profile.

Leo: That one I don't get at all.

Steve: I don't want - yeah, I don't want bitly changing my profile.

Leo: I can't think of any reason why they would want to.

Steve: So here's the problem we have. Okay, now, these are rights that bitly asked Twitter to grant. And what would be nice, and frankly I'm ashamed I don't know the OAuth protocol off the top of my head to know whether it's possible for Twitter to downgrade the rights it returns. I don't remember now the way the protocol works. But it would be nice if Twitter said, well, it would be nice if bitly only asked for what it really needs. And I think it's asking for more than it needs through OAuth. Clearly this is what happened to the other guy, assuming that he didn't fall for the first hack that you outlined, Leo. What happened to that guy was the same thing here. That site asked for everything. Twitter said, "We're going to give him everything, okay?" And he said yeah, okay.

Leo: This is a problem. It's a problem on Android, too. It's kind of permissions fatigue because all of these places, when you - Android does this, too. It gives you a long list - this is why I like Apple's approach, the intense - the way Apple's going to do this. But that gives you a long list of things that the app wants permission to do. And nobody reads that. They go yeah, yeah, yeah, yeah, yeah.

Steve: Although, right, the Apple guys are going to go through and audit those rights and say, wait a minute, why do you need clipboard access? You're not doing anything with a clipboard.

Leo: Yeah, yeah.

Steve: Yup. So...

Leo: I think that's Apple's approach and is the sensible approach. But not everybody can do that.

Steve: Yeah. So what I would say to people is when - and here's the problem is, as a user, I have no control. OAuth, I mean, sorry, bitly is saying it wants these things. Twitter, when I go, when I bounce over to Twitter's site to give permission, they're being enumerated, but I have no way to say, uh, no on this and no on that and no on that, at least in this particular Twitter case. And again, I don't know whether the protocol allows it or not. So I can either say yes or no. Either I have no access that way, or I do. I mean, and bitly isn't allowing me to authenticate otherwise. So I don't know. We need more granularity of control, at least in this particular authentication loop.

Finally I just - we're nearing the end here and approaching an hour and a half of podcast. So I was right that we would not have time to get to any other content. I got a kick out of the fact that RIM has updated their PlayBook to thwart the jailbreaking that...

Leo: No.

Steve: ...Dingleberry was doing.

Leo: Dingleberry?

Steve: Dingleberry for the BlackBerry, yeah. But Dingleberry for the PlayBook, it was exploiting a flaw to allow jailbreaking, giving users root access and allowing them, among other things, access to the Android Market.

Leo: So, come on. Nobody's buying that piece of crap anyway. Might as well let them hack it.

Steve: So RIM...

Leo: You'll sell more, RIM.

Steve: That's really true. RIM updates the PlayBook to close the flaw and prevent Dingleberry's access.

Leo: E. Karchinski [ph] in our chatroom says, that one guy who bought a PlayBook can't jailbreak it now? Come on.

Steve: Within hours, Dingleberry...

Leo: Yeah. They cracked the crack.

Steve: ...updated themselves, simply using a different flaw, and they're back to it again.

Leo: I'm sure there's no lack. Dingleberry.

Steve: So, nope. I just wanted - I am approaching another milestone that I saw the other day and made a note. We're approaching 90 million uses of ShieldsUP!.

Leo: Wow.

Steve: When I looked this morning, I think it was, we were at 89,961,921. So...

Leo: That's not sales, that's people. So you somehow record....

Steve: Oh, I wish that were sales. No. No, that's not...

Leo: You'd be a billionaire.

Steve: I don't have 90 million.

Leo: But you record somehow - come on, Steve. You record when people use SpinRite?

Steve: You know me better than that. No. I have an MRU list, that is Most Recently Used list, of one - it's 1K long. So it's actually 4K bytes. 1K, the most recently 1,000 IPs that ShieldsUP! has...

Leo: Oh, ShieldsUP!. Not SpinRite, ShieldsUP!.

Steve: ...not SpinRite, has acquired.

Leo: Got it.

Steve: And so while people bounce around GRC, I'm not double counting them. They have to go away long enough to be flushed out of that MRU list. And then when they come back, typically a day or two later, or a month or two later, whatever, I count them again. So that's a very good count. That's 90 million people, essentially, have used ShieldsUP!.

Leo: Nice.

Steve: We'll have a party when get to a hundred million. But at this point we're 90 percent of the way there.

I already mentioned SGreads, which is my new Twitter feed. Anybody who thinks they might be interested, the first posting there is an interesting article from a day or two ago I really thought was thought-provoking, titled "How Doctors Die."

Leo: Ooh.

Steve: And it said that doctors don't die the way the rest of us do because they know better than to keep themselves alive past the point that it makes any sense. So...

Leo: Oh, that's interesting. So a lot of suicides.

Steve: No, no, no. Well...

Leo: I'm sorry. I shouldn't - that's a bad assumption. I'm so sorry.

Steve: Not a lot of suicide. But, for example...

Leo: They just say, "I'm done." No.

Steve: It would be, yes, we could...

Leo: We could prolong this, but let's not.

Steve: We could prolong this for another week by putting horrible things into your body. The example that was drawn was actually one of issuing CPR and breaking all your ribs when you're elderly because apparently CPR performed correctly does break your ribs.

Leo: Breaks your ribs. But it keeps you alive. No, I have that "Do Not Resuscitate" thing on me. Jennifer and I have a deal. We're going to put a pillow on each other's faces when it comes to...

Steve: Actually, Leo, I have to say it's the first thing, it's the first reason I ever considered getting a tattoo.

Leo: Oh. Good idea. Just write on your forehead, "Do Not Resuscitate."

Steve: Well, I wasn't going to go for my forehead.

Leo: Well, what? Your butt? I mean, where do they - it's got to be somewhere they're going to look.

Steve: Maybe on my chest.

Leo: Right there. Do not - oh, yeah, right where they would - yeah.

Steve: It turns out it would be either "DNR" you would tattoo, or apparently a lot of doctors actually wear bracelets that say "No Code." And "No Code" is what the...

Leo: Like Code Blue, Code Red...

Steve: Exactly. Which is to say, if I'm dead, leave me there, rather than bring me back. So...

Leo: But is that legally binding, if you just put - by the way, Dr. Mom says - and again, Dr. Mom, who is apparently now the most cited person ever in the history of TWiT, says, because she's a physician, says put it in your armpit. She doesn't explain.

Steve: Okay. I guess you've got to stay shaven, then, too, in order to...

Leo: But here's the - or your inner - but here's the question. Does that have the force of legality? I mean, is it a DNR? I mean...

Steve: Good question.

Leo: Aren't they going to ask your next of kin?

Steve: Don't know.

Leo: I might do that. I think that's good. "No Extreme Measures" or "No Code." It's not that - not "Do Not Resuscitate." Look, if I passed out on the sidewalk, it's okay to give the kiss of life, especially if you're a beautiful young woman. But...

Steve: And what's a few broken ribs between friends?

Leo: Right. But no extreme measures.

Steve: Yeah.

Leo: Yeah.

Steve: Anyway, it's an interesting article.

Leo: I like that.

Steve: I commend our listeners to it, if they're interested. And when I find things from time to time - and again, it won't be a high volume feed. None of mine are. But SGreads is where I will put them. And I wanted to mention that iBook recently got updated to v1.5 with two very welcome improvements.

Leo: Yes?

Steve: You get to it with the Font button on the UI. One is full screen, that removes that ridiculous book-binding border.

Leo: Oh, thank god.

Steve: I know. It's like, okay, a little too cutesy by half, Apple, thank you anyway. And also there's a nighttime mode that inverts the screen so it's very gentle white text on a black background and is much easier on your eyes if you're reading in a low-light situation. It's not nearly as glary. And in fact, back when I was reading on my Palm Pilot, I used the invert-the-screen feature of an old reader back in the day and really enjoyed reading that way.

And I thought I would close with a nice mention of SpinRite, which we haven't sold any of recently.

Leo: What?

Steve: No, because we seem to be scaring...

Leo: Oh, yeah, that's right, you had a slow weekend, that's right. No yabba-dabba-dos because of the SSL.

Steve: Yeah, Fred Flintstone is lonely. But someone whose initials are P.P.S. said, "I've been a SpinRite customer since v5. I've been using it occasionally but have had no real problems with my hard drives. I was glad to have the product, but until last night I couldn't actually say it worked, as I had not encountered any drive problems." Well, of course that's one of the benefits of using it occasionally is it'll prevent you from having drive problems, which is absolutely true. He said, "I have recommended the product to others based on my satisfaction with your freeware tools, assuming that your commercial product was good, too. That has now changed."

Leo: What?

Steve: "For the past week or" - no, no, meaning that, well, here it goes.

Leo: Okay, yeah.

Steve: "For the past week or two, I've been noticing that when starting Windows it would almost boot up, but would not display the list of users to select. Sometimes I would see the users, but would be unable to mouse over to them to enter the password. It got to the point that I would sometimes have to boot three or four times to get a good boot. I was thinking a Windows reinstall was going to be required. Knowing how long that would take just to do the install, let alone to reinstall my favorite applications, I thought I'd run SpinRite, just in case the problem was not corrupted files, but rather an inability to read the data. I ran SpinRite on my boot and C: partitions overnight. Since then I have had no further reboot issues at all. I can now recommend the program to others with the full knowledge that it really does work, and it saved me many hours of tedious Windows install blues. Good job. P.P.S."

Leo: I take it that that drive did not have "DNR" written on it. Can that - is that going to - could that ever - no, that wouldn't happen.

Steve: No.

Leo: Do not resuscitate this drive. No extreme measures. SpinRite is Code Blue for hard drives.

Steve: Exactly. Anybody who's inclined to purchase it, don't be put off by the fact that you may get a warning from Certificate Patrol.

Leo: That's a good thing.

Steve: In this case, we have more security than we ever have before.

Leo: Spin.pdf. So I've been busy during this show, and I hope you don't mind, every once in a while I do some things. And we got our stack of Christmas cards, and we're sending them out, and I've been signing them as we've been talking.

Steve: Ah.

Leo: Paying attention. It's like knitting.

Steve: Nope, I appreciate that, Leo.

Leo: Yeah. You'll get one. But I just thought it'd be kind of fun because this is this year's Christmas card, "Happy Holidays from the TWiT Brick House." And inside we have all the people who are on the front. There's 19 people on the front. And I just thought, and I asked Frederica, and she had last year's, and we went from, let's see, that's one, two, three, four, five, six, seven, eight, nine, 10, 11, 12, 13. So we added six people, almost a 50 percent growth this year. Which is all right because we had a 40 percent growth in revenue. So that kind of is - kind of works out. And most of these people are still here. I think. Becky, Becky's moved. It's kind of, you know, she's emeritus. But she'll be back. Anyway, I think that was kind of fun, to see this is in front of the old cottage, that's last year's card. And this year's card is in the new brick house studios.

Steve: Very nice.

Leo: Yes, they're festive. Well, you'll get one of those.

Steve: Cool.

Leo: So, Steve, next week Tom Merritt'll be back because I'll be on vacation. Then I'm coming back for a very special Security Now! on the 27th. It will come in your Christmas package, your downloads: Steve's Sci-fi Episode, where we don't talk security, we just talk reading.

Steve: Unless something really horrible happens.

Leo: You know it will.

Steve: Yeah. So, I mean, maybe we'll do security. But the show's intent, our content, this is the Special Holiday Science Fiction Episode.

Leo: You know what I should get, I should get a short, very, very short sci-fi story we could read out loud or something. That'd be kind of fun. 'Twas the night before Alpha Centauri.

Steve: Actually, Leo, we're going to have so much to talk about.

Leo: Oh, okay.

Steve: We're going to have so much to talk about...

Leo: Good.

Steve: ...I don't think we're going to need any more, so...

Leo: And I did suggest - somebody's saying in the chatroom you should get Tom on for that. Replicant says you should get Tom on the thing. Of course, Tom and

Veronica Belmont do a sci-fi podcast called Sword and Laser.

Steve: Well, see, but, okay. If it's hard sci-fi, I'm all for it. But not any...

Leo: No, they do fantasy. Yeah, they do unicorns.

Steve: Yeah, see, that's not science fiction. I don't know why people put those together. But unicorns have no place.

Leo: I'm kind of with you on that. No fantasy for me.

Steve: I want phasers. I want teleportation. I want light speed. I want warp cores. I want...

Leo: Flying cars.

Steve: Yeah, you betcha.

Leo: Steve Gibson is at GRC.com, the Gibson Research Corporation. GRC.com is where you'll find SpinRite, the world's best hard drive maintenance and recovery utility, and all his other freebies, too. And there are a ton of them. And Steve, our chatroom, our intrepid chatroom has done a little research. And there at GRC.com is the picture that Consumer Reports got from GRC.com/stevegibson.htm. It's your own...

Steve: Oh, on my own page.

Leo: It's your own picture.

Steve: Yeah, and I've got to update that, I guess, yeah.

Leo: Associated Press Photo by Krista Niles, April 12th, 2002.

Steve: Yup.

Leo: A little less gray.

Steve: Oh, a lot less gray. And more hair. Or less hair, also.

Leo: "My Little Corner of the Web" is the name of that.

Steve: Ah. Well, good researchers.

Leo: You cannot put one past our chatroom. I can tell you that right now.

Steve: Nope.

Leo: Have a great...

Steve: We're done.

Leo: ...holiday. I'll see you on December 27th. We're done. Thank you, Steven.

Steve: Oh, that's right, I'm not going to see you next week. So in two weeks you'll be back for the sci-fi show.

Leo: Yes. Merry Christmas.

Steve: Perfect. Thanks, my friend.

Leo: Thanks, Steve. We'll see you next time on Security Now!.

Steve: Bye.

Leo: Bye.